

链基治理：即将到来的全球电子社会契约

杨 昊

内容提要：分布式存储和分布式预言机技术的成熟标志着区块链正在不断克服性能瓶颈和数据联通瓶颈，从而为链基治理奠定技术基础。全球治理中的链基治理意味着为全球治理提供一份具有自执行能力的电子社会契约，这一契约对全球治理多元行为体带来了不同的机遇和挑战。对于国家来说，应对全球电子社会契约的关键在于掌握区块链的自治理，掌握自治理的核心在于对共识机制的把握。通过链下治理作用于区块链的自治理，进而驾驭链基治理，构成区块链治理的国家路径。

关键词：区块链 共识机制 全球治理 社会契约 全球学

区块链（Blockchain）技术最早应用于加密数字货币，因此其常被视作一个电子账本。究其实质，区块链是一个共享数据库。当用于记录货币交易时，区块链发挥了账本的功能；当被应用于记录物品所有权时，区块链可以成为一份不可更改的所有权证明。区块链不仅可以记录信息，通过共识机制（consensus mechanism）设计，这一数据载体还具备了价值交换的功能。传统上，在排除面对面交易的情况下，价值交换只能依靠第三方的信用背书来实现，区块链则可以在不依赖第三方中间机构的情况下实现价值交换，这就使得该技术不仅可以记录货币或所有权信息，还可以实现货币流通和所有权的转让、交易。特别当智能合约出现后，区块链上的价值交换具备了前置的自执行能力，一旦触发合约条件，价值交换将自动完成。当价值交换的内容不再局限于数字货币和有形

杨昊，中国政法大学全球化与全球问题研究所副教授。本文为国家社科基金青年项目“区块链共识机制对全球治理规则制定的启示研究”（21CGJ013）阶段性成果。

资产所有权，而扩展至更广泛的公共记录、各种无形资产以及准入身份等内容时，区块链开始适用于更加广泛的应用场景。当区块链能够在更加广泛和复杂的应用场景中，对各种价值交换合规地行使自动执行能力时，该技术也就衍生出了社会强制力，进而具备了作为各种分布式自治组织（Decentralized Autonomous Organization, DAO）的技术基础，成为一份电子版的社会契约的可能性。

关于区块链的政治经济学讨论受到该技术发展阶段的影响。2009—2013年，区块链技术出现以比特币的诞生和一系列其他加密货币的出现为标志的第一波发展浪潮；2014年至今，区块链技术迎来了第二波发展浪潮，随着智能合约的出现，区块链作为分布式自治组织基础设施的潜力开始显现。¹ 受到这两波发展浪潮的影响，有关区块链治理（blockchain governance）的讨论主要沿着两个方向展开：一是“对区块链的治理”（governance of blockchain）。当区块链主要发挥信息记录和价值交换功能的时候，区块链治理通常指的是对这一技术及其应用的治理。比如对以比特币为代表的数字货币及其金融后果的治理，其治理工具通常诉诸技术以外的制度、法律和社会规范等，因而这一类治理也可称为“链下治理”（off-chain governance）。² 二是“由区块链治理”或“借助区块链治理”（governance by/with blockchain），指当区块链和智能合约结合施之于各种社会组织，并发挥社会契约的功能时的治理，又称“链基治理”（blockchain-based governance）。这种情况下的治理通常借助对区块链共识机制的设定，让分散的节点达成集体行动，以对信息进行记录、验证和监督，借助智能合约推进价值交换，进而让区块链成为服务于特定集体目标的底层技术支撑，因而这一类治理也被称为“链上治理”（on-chain governance）。³

链下治理和链上治理是关注区块链与治理，特别是与全球治理关系的文献的主要关切方向，这两种治理的共同点在于关注新兴技术与其所处社会之间的关系：或是运用各种社会条件以区块链作为治理对象，或是将区块链技术施之于社会管理。此外，一种更具技术色彩的区块链治理也开始成为研究者的关注焦点，即区块链的“自治理”。与前述两种区块链治理的不同点在于，区块链的“自治理”与链外社会之间并不具有直接因果关系，但却可以作为连接链下治理和链上治理的桥梁，并间接与社会条件发生关系。马尔科姆·坎贝尔-韦杜因（Malcolm Campbell-Verduyn）对“由区块链治理”和“借助区块链治理”之间的差别进行区分，认为尽管两者都强调区块链技术的社会意义，前者反映了一种基于刚性的

1 David Rozas, et al., “When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance,” *SAGE Open*, Vol. 11, No. 1, 2021, p. 2.

2 Wessel Reijers, et al., “Now the Code Runs Itself: On-chain and Off-chain Governance of Blockchain Technologies,” *Topoi*, 2018, pp. 1-11.

3 Wessel Reijers, et al., “Now the Code Runs Itself: On-chain and Off-chain Governance of Blockchain Technologies,” *Topoi*, 2018, pp. 1-11.

预编程电脑代码的治理，而后者则通过对区块链的设计实现对特定权力关系的巩固。例如，当前主流区块链的核心团队通常集中在发达国家和地区，并且将他们的偏见和对世界的看法植入所谓的中性技术设计中。¹ 坎贝尔-韦杜因在此处提及的“借助区块链治理”，实际上将关注焦点放在了区块链核心社区的特征和以共识机制为代表的代码设计上。维塞尔·雷耶斯（Wessel Reijers）等人在对区块链治理进行链上和链下的区分后，进一步将链下治理区分为内生规则和外生规则两类。其中，内生规则特指区块链社区为实现系统的正常运行和持续发展所采用的规则，包括对共识机制的执行和修改。² 类似地，罗文·范佩尔特（Rowan Van Pelt）等人在一篇以区块链为治理对象的论文中，将链下治理区分为两层，一层指向外部社会条件，一层指向区块链社区内部的互动和决策过程，此外增加一层链上治理，特指以区块链共识机制为代表的代码设计对区块链自身治理的意义。³ 因此，链上治理和链下治理可以各自分出一个内生向度，指向区块链社区和应用的自治理，其中包含社区不同成员之间的互动关系（链下），并反映在以共识机制为代表的代码设计中（链上）。区块链治理的内生向度具有连接外向的链上治理和链下治理的功能：外部社会的规范、法律和制度等通过对区块链社区及其共识机制进行治理发挥影响，区块链社区及其共识机制又成为该技术影响外部社会的基础。

据此，本文将区块链治理区分为三部分：链下治理（特指外生社会规则对区块链的治理）、链基治理（特指区块链技术对社会治理的外生影响）以及区块链的自治理（包括了内生的链上和链下治理），参见表1。

表 1 区块链治理的分类

	链上	链下
外生	链基治理	链下治理
内生	区块链的自治理	

资料来源：作者自制。

虽然链下治理作为当前区块链治理的热点问题，给传统的社会和互联网治理提出了紧迫挑战，但链基治理在全球治理中具有潜在的革命性意义。在全球治理中运用链基治理，意味着为全球治理定下具有自执行能力的全球电子社会契约，

1 Malcolm Campbell-Verduyn, eds., *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*, New York: Routledge, 2018, pp. 185-186.

2 Wessel Reijers, et al., “Now the Code Runs Itself,” pp. 1-11.

3 Rowan Van Pelt, et al., “Defining Blockchain Governance: A Framework for Analysis and Comparison,” *Information Systems Management*, Vol. 38, No. 1, 2021, p. 30.

运用链基治理技术,意味着为全球治理定下具有自执行能力的全球电子社会契约,从而提供一种超越市场和公共管理的导向共同利益的新治理方式。

从而提供一种超越市场和公共管理的导向共同利益的新治理方式。¹ 随着区块链分布式存储和分布式预言机为代表的技术不断发展,链基治理面临的性能瓶颈和数据联通瓶颈正在被打破,基于该技术的全球电子社会契约有望成形。如果全球治理可以建立于全球电子社会契约的基础上,那么当前全球治理面临的低效、分裂局面有望得到修正,以应对全球问题带来的越来越紧迫的挑战。本文将在结合区块链技术最近发展趋势的基础上,论述一种电子社会契约版的全球治理对国际组织、国家和非政府组织等多元行为体的潜在影响,并

进而指出,对于国家来说,驾驭链基治理的关键在于通过链下治理实现对区块链自治理的把握,而自治理的核心反映在共识机制的设计上,从而为国家借助该技术引领全球治理发展提供一些思考。

一、迈向全球电子社会契约:区块链分布式存储和分布式预言机

链基治理建立在区块链发挥社会契约功能的基础上。如果说社会契约论只是政治哲学中的思想实验,那么智能合约赋予区块链的价值交换自执行能力和无界的分布式网络,则让其有可能成为全球范围的电子社会契约。链基治理和现存国际机制间的一个重要区别,在于前者是分布式网络,而后者是中心化的机构。虽然分布式网络避免了与中心化机构相伴生的单点脆弱性,但其在确保安全性的同时,却不得不以性能上的牺牲为代价。因此,如果增加分布式系统的可扩展性,则其安全性将会降低;除非放弃分布式系统,否则安全性和可扩展性难以同时兼顾。1998年,加州大学伯克利分校的计算机科学家埃里克·布鲁尔(Eric Brewer)提出分布式系统的CAP理论,该理论认为,在一个分布式系统中,很难同时兼顾一致性(Consistency)、可用性(Availability)和分区容错性(Partition Tolerance)。² 区块链作为一个分布式系统,面临着类似的“三元悖论”,即安全性、效率(可扩展性)和去中心化(分布式网络)难以同时兼顾。从最早的区块链应用——比特币开始,确保安全性和分布式网络的考量就优于可扩展性的考量。截至目前,比特币每秒可处理交易量为7笔,最大的具有智能合约功能的公共区块链开源平台以太坊(Ethereum),每秒可处理交易也在30笔以下,相较而言,中心化的维萨(VISA)信用卡每秒交易量最高可超过60000笔。在应用到更广泛的社会管理事务中时,区块链在可扩展性上的局限将让全球链基治理成为难

1 David Rozas, et al., “When Ostrom Meets Blockchain: Exploring the Potentials of Blockchain for Commons Governance,” *SAGE Open*, Vol. 11, No. 1, 2021, p. 1.

2 Seth Gilbert and Nancy Lynch, “Perspectives on the CAP Theorem,” *Computer*, Vol. 45, No. 2, 2012, pp. 30-36.

以企及的乌托邦。此外,区块链本身是一个封闭系统,将其运用于全球治理时,必须解决如何高效及时地将外部信息引入区块链系统,实现链下信息与链上合约沟通的问题。克服可扩展性难题,以及与链下信息的联通问题,是区块链走向全球社会契约所必须应对的挑战。从2020年下半年开始,分布式存储和分布式预言机技术发展迅速,正在从技术角度突破链基治理的瓶颈。

(一) 分布式存储与区块链性能扩展

从2020年下半年开始,区块链分布式存储项目开始成为区块链应用中的快速增长点,出现了STORJ(2017年启动)、FIL(2020年启动)等一批有代表性的应用落地项目,截至2021年8月,分布式存储领先项目FIL发行的数字货币“filecoin”市值已超过74亿美元,¹ STORJ接近6亿美元。² 区块链分布式存储是星际文件系统(Internet Planetary File System, 以下简称为“IPFS”)和区块链技术结合的产物。³ IPFS是自2014年出现的对标超文本传输协议(HTTP)的分布式文件存储协议,与依赖因特网主网和各种集中化服务器的超文本传输协议不同,星际文件系统是去中心化的点对点分布式文件系统,该协议将文件数据进行分片(sharding),⁴ 分布式地存储在多节点的硬盘设备中,并借助加密技术确保文件安全。星际文件系统和区块链技术的结合意味着区块链正在克服一个阻碍其成为更广泛社会契约的性能瓶颈。

区块链可扩展性上的限制带来三个问题:其一是链上信息容量受限,这一点在比特币上表现得非常明显。为了保证系统的安全性,每一区块的容量被限制在1兆字节左右,即使在采取隔离见证(Segregated Witness, 简称“SegWit”)技术后,⁵ 区块容量也仅为2兆字节以内。为了安全性所做出的容量牺牲,限制了区块链的可扩展性。其二是信息记录的成本过高。当区块链的容量限制了交易流量时,矿工费用将成为信息竞争被记录的重要方式,从而推高区块链记录信息及执行智能合约的成本。为了激励矿工的工作,矿工费用更高的交易将被优先处理,随着区块链信息吞吐量的增加,矿工费用的竞逐造成了区块链交易成本的大幅攀升。其三是数据库文本体量过大,去中心性受到侵蚀。作为一个分布式账本,区块链要求信息被记录在节点的存储空间之中,随着账本容量的不断增长,普通节

1 代币市值(CoinMarketCap)网站: <https://coinmarketcap.com/currencies/filecoin>, 2021年11月5日登录。

2 代币市值网站: <https://coinmarketcap.com/currencies/storj>, 2021年11月5日登录。

3 Protocol Labs, “Filecoin: A Decentralized Storage Network,” p. 1, <https://filecoin.io/filecoin.pdf>, 2021-11-05.

4 STORJ Labs, “Storj: A Decentralized Cloud Storage Network Framework v3.0,” pp. 36-39, <https://www.storj.io/storjv3.pdf>, 2021-11-05.

5 隔离见证是比特币采用的扩容方案,做法是提取原本存放在区块中的交易签名并放到外部,这样交易区块内部就能存放更多的交易记录,间接达到扩容目的。见李洋等:《区块链扩容技术研究综述》,《电力信息与通信技术》,2020年第6期,第4页。

点将难以承担复制全账本的任务。以比特币为例,一个复制所有账本信息的全节点(full node)所需保存的数据已超过300千兆字节,以太坊则超过了5太字节,且账本数据仍在持续增加。尽管只有全节点才需备份完整账本,但不断增加的数据容量仍然在不断抬升全节点的门槛,对区块链的去中心性造成威胁。

分布式存储是对上述瓶颈的重要突破,该技术借助分片的方式实现对区块链的扩容。所谓分片,就是通过将数据分割成多个更易处理的小数据从而提升处理性能的扩容技术。¹ 星际文件系统技术与区块链的结合,意味着系统仅需将数据对应的加密哈希(hash)和相应时间戳存储到链上,而庞大的数据本身则被分布式存储到节点硬盘空间中,从而极大缩减区块链数据库规模、解放区块链空间,降低交易费用。分布式存储的快速发展,为区块链作为全球电子社会契约奠定了效能基础。

(二)分布式预言机与链下信息上链

分布式预言机同样是2020年下半年以来的区块链项目增长点。如果说分布式存储是为全球电子社会契约打下更深的地基,那么分布式预言机则是在扩展这份契约的广度。区块链本身是一个封闭系统,智能合约无法直接与链下信息相联通,如果将该技术应用于更广泛的社会事务治理,则必须将链下信息和链上合约相联通,也就是将电子版的社会合约和此前已经存在的现实世界数据相联通。特别是当治理对象涉及大量且不断变动的数据时,区块链需要依赖链下专门机构提供信息资源,并将其传导到链上以触发智能合约,实现信息从链下向链上传导的工具,即为预言机(Blockchain Oracle Machine)。

预言机本身并不是新事物,但传统中心化的预言机无法满足链基治理对分布式系统和安全性的需要,倘若在信息转移过程中需要通过中心化的预言机,这就意味着预言机有可能操弄数据。区块链的重要价值体现在去中介化上,但链上和链下信息的沟通又不得不通过预言机这一中间过程,因此,一个分布式而非中心化的预言机网络便成为链基治理的良方。2014年,分布式预言机网络ChainLink正式启动。经历了一段时间的蛰伏后,ChainLink区块链项目在2020年开始引人关注,截至2021年8月,其代币Link市值已超过140亿美元。² 作为第一个去中心化的预言机网络平台,ChainLink通过将经过验证的链下数据聚合发送到区块链上,从而触发智能合约的自执行,借助分布式网络和信息提供节点的声誉评估机制,保证数据在传播过程中的去中心性和可信性。³

1 曹雪莲等:《区块链安全、隐私与性能问题研究综述》,《计算机集成制造系统》,2021年第7期,第2087页。

2 代币市值网站: <https://coinmarketcap.com/currencies/chainlink/>, 2021年11月5日登录。

3 Lorenz Breidenbach, et al., "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks," Chainlink Labs, <https://research.chain.link/whitepaper-v2.pdf>, 2021-08-12.

当区块链的性能瓶颈和信息闭环瓶颈被打破时，基于区块链技术的全球电子社会契约就具备了更坚实的基础，也预示着链基治理未来可期。

二、链基治理对全球治理多元行为体的挑战与影响

全球治理作为由多元行为体共同参与的全球集体行动，因其在权责划分和行动效率上没有发挥有效作用而饱受诟病。除了构建“世界政府”和放弃全球治理这样的激进观点以外，如何规范多元行为体的行动、如何安排全球公共物品的融资和分配以及如何设定治理机制的权责，成为全球治理研究的“西西弗斯”神话，成效甚微又永不停止。不断恶化的气候条件、突然暴发的公共卫生危机等当代全球问题与低效全球治理之间的矛盾越发突出。链基治理可通过引入一份具有自执行能力的全球电子社会契约，为全球治理的推进带来新的希望。

与全球治理实践相结合，伯恩哈德·莱斯贝格（Bernhard Reinsberg）对链基治理在气候变化议题中的应用场景进行设想。他设计了一个包括国家、国际组织、非政府组织和专家共同体在内的许可链形式的分布式自治组织。在其中，以国家自主贡献（Nationally Determined Contributions, NDCs）为代表的键数据将被披露并且不可修改地记录在区块链上，形成透明信息，从而降低以联合国气候变化框架公约（UNFCCC）秘书处为代表的中心化机构记录信息所带来的行政成本，并且避免双重计算，降低对碳排放行为的监督成本。此外，与物联网和预言机的结合，将让气候变化相关信息的获取渠道更加准确和丰富，智能合约和投票系统也有助于国家对气候治理的规则进行调整。进一步，国家可以选择将这一许可链和其他区块链连接起来，扩展成一个开放的区块链生态系统，通过发行数字货币，实现气候治理多重任务的互操作性。比如，任何行为体都可以通过减排行动获得数字货币，并且将其反用于支付碳排放费用，数字货币既可以用于鼓励个人的减排和信息提供行为，也可以用于对在能源产业转型中利益发生变化的人群进行调整和补偿。在国家层面，数字货币则可以用于对国家减排承诺进行奖惩。¹ 当国家将资产映射到数字货币体系中后，自动执行的智能合约将对国家资产进行增减或再分配，从而强化全球治理的效力。²

社会契约论是政治哲学家思想实验中的产物，帮助人们理解公共权力的起源、性质、与公民的关系以及应当如何发展等问题，区块链技术有可能让这种思想实验中的产物变为全球层面的现实。有研究者认为，区块链综合反映了社会契约论者的不同观点。对人性持悲观态度并借助智能合约实现高效执行力的理念与

1 Bernhard Reinsberg, "Fully-automated Liberalism? Blockchain Technology and International Cooperation in an Anarchic World," *International Theory*, Vol. 13, No. 2, 2021, pp. 296-298.

2 高奇琦：《主权区块链与全球区块链研究》，《世界经济与政治》，2020年第10期，第63页。

霍布斯对原初状态和利维坦的设定相接近;对由人组成的中间机构的不信任并且用分布式网络的方式重建信任的做法则接近卢梭对于原初状态的假定和对激进民主的规划;技术面前人人平等的设想则接近于罗尔斯“无知之幕”(veil of ignorance)的观念。¹

设想当前全球治理存在一个社会契约,这一契约用于规定行为体的权利义务并导向实现善治。尽管现实世界中并没有形成一个完整规范的文本,但在各种国际组织的宪章、声明和专门机构的研究报告中,仍然可以觅得这一契约的踪迹,它既涉及人类整体安排,如《联合国宪章》和全球治理委员会的报告,也涉及和人类未来有关的各议题领域,如《国际卫生条例》和政府间气候变化专门委员会(IPCC)的报告。这些碎片式的契约主要由国际组织执行,由跨国倡议网络监督推动,并受到国家意愿的制约。将区块链作为全球治理的社会契约,意味着将一种刚性的执行机制和分布式的民主意见表达机制引入全球治理,取代已有的碎片化和柔性的治理契约,这必然给不同行为体带来不同的挑战。

首先,具有中介功能的各种政府间国际组织和非政府组织将面临功能被替代的挑战,进而受到功能转型的压力。对于自由制度主义者来说,以国际组织为代表的各种国际机制维系了国际秩序的稳定,在一定程度上取代了霸权国的功能,²这种功能既包括跨国事务的执行功能,也包括为国家提供关于未来的稳定预期的功能。

区块链技术的核心思想是去中心化,中心指的是发挥中介功能的各种机构,中介机构在资源和信息的调配过程中成为中心。在跨国事务中,国际组织在资源和信息的调配过程中需要获得国家的授权和同意,仅在一定程度上发挥了中心作用,但其无疑是中介机构。如果一份基于区块链的全球电子社会契约成为现实,受到影响的首当其冲的就是在全球集体行动中发挥中介作用的国际组织。从执行方面看,链基治理相较于传统的国际组织具有自动执行的优势,这种优势源于智能合约的强制力前置。³与现实世界中的各种国际机制不同,链基治理在进行全球治理的时候,将基于事前制定好的合约执行规则,从而避免国际机制在执行国际规则时受到强权的干扰。国际组织的一大弊端在于执行力低下,无论积累了多少成功的实践,只要大国的意愿发生扭转,国际组织就要面临失去执行力或丧失独立性的挑战。换句话说,国际组织强制力的每一次发挥都需经受国家意愿的考

1 Weissel Reijers, Fiachra O'Brolcháin, Fiachra and Paul Haynes, "Governance in Blockchain Technologies & Social Contract Theories," *Ledger*, Vol. 1, 2016, pp. 134-151.

2 [美]罗伯特·基欧汉:《霸权之后:世界政治经济中的合作与纷争》,苏长和等译,上海:上海人民出版社,2006年版。

3 Primavera de Filippi, "Blockchain Technology as an Instrument for Global Governance," SciencesPo, September 2020, <https://www.sciencespo.fr/public/chaire-numerique/en/2020/09/11/primavera-de-filippi-blockchain-technology-as-an-instrument-for-global-governance/>, 2021-08-12.

验。智能合约的运用则将这种强制力前置,一旦条件满足,将会自动触发合约,从而降低国际组织强制力执行的国际政治难度。此外,自执行的价值还体现在协调国家行为体之间的关系上,这种协调可以通过区块链的价值转移功能实现。通过价值转移可建立国家间的可信的补偿制度,有助于降低国家合作的潜在风险,为有合作意愿的行为体提供更具确定性的未来预期,激励国家采取行动。¹当链基治理在执行和提供稳定预期方面优于国际组织时,后者就面临着转型的压力。

对于建构主义者来说,国际组织依靠理性-合法权威获得基本形式,依靠授予性权威、道义性权威和专家权威服务于特定的社会目的,从而发挥“为世界定规则”的作用。²其中,理性-合法权威源于国际组织作为非人格化的官僚机构在跨国事务中行使中间和中介功能,链基治理的去中心化和信息的不可更改性将让国际组织的该类权威受到冲击。此外,国际组织的专业性权威也将在汇集了分布式预言机技术,从而拥有充分信息来源的链基治理面前受到挑战,进而影响国际组织的授予性权威的获得。当国际组织多样的权威来源受到挑战时,其在“构建社会事实中的决定性优势”³也将不复存在。国际组织未来的着力点将会是道义性权威和更集中且可信的专业性权威,并且其将借之强化授予性权威,重塑理性-合法权威的方向。换句话说,在未来的全球电子社会契约中扮演契约维系者、监督者以及价值倡导者的功能,将成为国际组织转型的方向。例如,在气候变化和公共卫生等涉及大量数据和专业建议的领域中,在分布式预言机中成为可信信息提供者,实现现实世界信息上链并对数据信息进行监督,以及确保具有道义性的治理目标的实现将成为国际组织的新的着力点。

在未来的全球电子社会契约中扮演契约维系者、监督者以及价值倡导者的功能,将成为国际组织转型的方向。

其次,相较于具有中介性功能的国际组织面临挑战的处境,以跨国倡议网络为代表的非政府组织和全球民间组织将在链基治理面前获得更多的机遇。与前一类国际组织不同,跨国倡议网络在全球治理中常常以监督者、倡议者而非中介的角色出现,这也导致这一行为体相较而言常处于边缘位置。链基治理的分布式共识及其带来的信息透明将赋予这一类行为体在扮演上述角色时更强的能力,而不是被阻隔在国家和政府间国际组织的圈子之外。甚至会发生这样一种情况,在链基治理的基础上,由于中心和中介的功能以及专业性的权威从国际组织转移向算法和技术,非政府组织和现有的政府间国际组织的功能发生趋同,规范塑造、信息监督和提供信息等领域成为这两者竞逐的场域。对于非政府组织来说,这种趋

1 Bernhard Reinsberg, "Fully-automated Liberalism? Blockchain Technology and International Cooperation in an Anarchic World," *International Theory*, Vol. 13, No. 2, 2021, p. 298.

2 [美]迈克尔·巴尼特、[美]玛莎·芬尼莫尔:《为世界定规则:全球政治中的国际组织》,薄燕译,上海:上海人民出版社,2009年版,第31页。

3 [美]迈克尔·巴尼特、[美]玛莎·芬尼莫尔:《为世界定规则:全球政治中的国际组织》,第43页。

势为其参与全球治理提供了重要的机遇。除以跨国倡议网络为代表的非政府组织外，以地方政府为代表的次国家行为体参与全球治理的门槛也被区块链降低。¹次国家行为体在全球电子社会契约前面临的门槛是读取和写入信息的权限，获得的是在分布式网络中进行价值交换的机遇。

最后，如果说在全球治理中受链基治理冲击最大的是发挥中介功能的国际组织，获益最多的是非政府组织和次国家行为体，那么国家则处于两者之间。刚性的全球电子社会契约，或是具有灵活性的传统国际机制，是摆在国家面前的选择，而国家的选择也是决定全球电子社会契约能否形成的关键。从国家的角度出发，一份具有自执行能力的全球电子社会契约实际上赋予了国家相对于国际组织更多的筹码，使国家在尝试推动全球治理时，有可能绕开低效且易受其他国家掣肘的国际组织，从而避免不确定性，但同时其自身的转圜空间也会受到限制。传统国际机制给国家的立场提供了灵活性，对灵活性的把控不仅意味着国家自身利益免于受损，同时也意味着强国有可能从模糊立场中获取更多的相对收益。链基治理的出现，不仅赋予国家相较于国际组织更多的选择，也收紧了其在全球集体行动中采取模糊立场的空间。

技术的不断成熟和全球问题的紧迫性，都在加快链基治理到来的步伐。对于国家来说，简单地拒绝或欢迎都不是明智的做法。在即将到来的未来挑战中，重要的是国家如何运用自身的合法性和实力去迎接链基治理，从而维护自身利益。其中，关键在于掌握区块链的自治理，而区块链自治理的核心则反映在区块链的共识机制中。

三、共识机制：全球电子社会契约的硬核

当国家在链基治理中尝试维护并扩大自身利益的时候，区块链的自治理就会成为国家的关切。其中，对区块链社区核心团队和智能合约的关切是国家维护利益的必要条件。共识层，也就是区块链的共识机制设计，则是国家驾驭链基治理的充分条件，能动性地掌握共识机制是国家的深层硬核筹码。

共识机制是区块链的核心底层算法，其作用是在区块链的分布式网络中让不同的节点达成一致。换句话说，共识机制旨在利用算法保证分散的行为体采取集体行动、实现合作，以保证区块链的正常运转。共识机制主要包括记账权的分配、数字资产发放和验证机制三部分。在链基治理的实践中，共识机制发

¹ Bernhard Reinsberg, "Fully-automated Liberalism? Blockchain Technology and International Cooperation in an Anarchic World," *International Theory*, Vol. 13, No. 2, 2021, pp. 287-313.

挥了社会规范和规则的作用。¹ 尽管共识机制创新层出不穷,但其主要由工作量证明(Proof of Work, PoW)、权益证明(Proof of Stake, PoS)、实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)等机制衍生而来。² 前述区块链存在的“三元悖论”,即很难同时实现去中心化(分布式网络)、效率(可扩展性)以及安全性,主要反映在共识机制的设计中。当前有代表性的共识机制都在保证安全性的前提下,对去中心化和效率进行了取舍。在链基治理的实践中,共识机制扮演了规则或宪章的角色,决定了相关全球治理的合作模式和治理参与者的权责分配。

(一) 区块链共识机制的构成:记账权分配、奖惩机制和验证机制

首先是记账权分配,主要包括工作量证明、权益证明和在许可链中广泛应用的实用拜占庭容错三种方式。工作量证明机制是由比特币开创的共识机制,并在早期被以太坊采用。区块链的记账权取决于计算机解密哈希密码的运算力,最先完成解密运算的节点将会获得记账权,即根据节点的工作量大小决定记账权分配。其优点是去中心化程度高,缺点是容易造成资源浪费且效率低下。权益证明机制是以太坊在工作量证明之后所采用的共识机制,其记账权取决于节点持权益的大小而非工作量,持有越多权益的节点将会获得越多的记账机会,从而提高了区块链的效率,减少了资源浪费,但该种共识机制的公平性较差,可能造成节点之间的“马太效应”,即强者越强、弱者越弱。在权益证明机制的基础上出现了委托权益证明(Delegated Proof of Stake, DPoS)机制,该机制可以被视作代议制在区块链中的运用,即在去中心化的节点中选举出一定数量的节点维系区块链系统的稳定运行,被选定的代表不仅承担监督的责任,还直接掌握着记账权。除上述广泛运用于公链的共识机制外,许可链相关共识机制是针对联盟链和私链所采用的共识机制。和对节点身份没有限定的公链不同,许可链对节点身份进行限制,通常被运用于有特定范围和较少行为体参与的治理事务中,如央行数字货币等。目前得到广泛应用的许可链共识机制是实用拜占庭容错机制,该机制对记账权的分配不取决于工作量或权益,而是将对记账权的分配委派给主节点,节点角色的确认方式可以是随机、投票或是指定。在记账权确定后,只要多数节点认可该节点的记账权和记账信息,共识即达成,尽管节点有可能共谋制造虚假认证,但其所有行动都被记录在案,可被追踪和溯源。实用拜占庭容错机制大大提高了区块链的效率,但其安全性受到冲击,对节点之间的互动信息量有极高要求,因

1 Stephen DiRose and Mo Mansouri, “Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations,” Paper Presented to the 13th Annual Conference on System of Systems Engineering, 2018, pp. 195-202.

2 Xiao Yang, et al., “A Survey of Distributed Consensus Protocols for Blockchain Networks,” *IEEE Communications Surveys & Tutorials*, Vol. 22, No. 2, 2020, pp. 1432-1465.

此适用于由较少行为体参与的治理机制。

其次是奖惩机制,主要包括数字货币和非数字货币两类。在工作量证明机制和权益证明机制中,区块链共识机制的奖励机制主要通过数字货币来完成,这也是数字货币的重要功能之一。获得记账权并得到验证的诚实节点将会获得数字货币的奖励,而不诚实的节点将会面临算力浪费和权益下降的惩罚。此外,一些新兴区块链在工作量证明和权益证明的基础上增加了质押要求,如质押证明机制(Proof of Mortgage, PoM),通过延迟发放全额数字货币或要求提前质押部分数字货币的方式,保证在节点造假时可没收质押物,从而施加惩罚。实际上,在有较少节点参与的许可链中,也出现了取消数字货币的共识机制,¹这些机制中的节点地位差异较大,依靠领导节点实施奖励或惩罚,不诚实节点面临被取消准入资格的风险。相较于工作量证明机制和权益证明机制,其容错性较小,取决于节点的数量和相互之间的信任程度,适用于有较少行为体参与的网络。

最后是验证机制,包括去中心化、多中心化和中心化三种方式。共识机制中的验证机制是对区块链上的交易信息进行监督的方式。在工作量证明机制和权益证明机制中,监督采取去中心化的方式。理论上,工作量证明和权益证明可以让网络中的每一节点都拥有监督记录行为的权利,并通过投票决定该区块是否合法,只要保证一半以上的节点是诚实节点,即避免51%的算力串谋造假,即可保证监督的有效。以委托权益证明为代表的共识机制,其验证主要由被选举出来的或特定数量的节点完成,被选举出来的验证节点类似于代议制机构中的立法者,其验证工作本身被全网监督。而在以实用拜占庭容错机制为代表的有较少行为体参与的许可链中,无须进行全网验证,只要特定数量的节点保持诚实,交易即可完成。此外,在一些许可链中出现了高度中心化的共识机制,特定节点被选择为监督节点,行使监督职能,由于验证中心化,其容错率变低,一般只适用于有较少节点参与的许可链。

(二) 区块链共识机制及其全球治理规则意义

在全球链基治理实践中,共识机制即为治理原则,这套原则将决定谁获得话语权,以及如何进行奖惩和监督。共识机制既是政策执行(智能合约)的前提,又是组织基础(密码学和点对点设计)的指导规范。因此,掌握共识机制是国家在链基治理中最为核心的任务。

首先,把握记账权作为全球治理话语权的意义。共识机制的重要任务是确认记账权的分配。共识机制设计的差异,最突出表现在记账权获得方式的差异上。获得记账权的节点,将会完成制造区块并记录信息的工作。在以区块链技术展开的全球治理实践中,记账权意味着对治理实践信息进行记录的权利。谁获得记

1 谭敏生等:《区块链共识机制综述》,《计算机工程》,2020年第12期,第9页。

账权将决定全球治理以哪种话语和叙事方式被记录。由于监督机制的存在,这种话语权并不意味着对全球治理的话语垄断,但仍然是避免不诚实节点获得话语霸权、串谋欺诈的重要手段。

其次,把握数字货币作为全球治理奖惩机制的意义。数字货币是鼓励节点完成区块制造并诚实记录信息的重要手段。共识机制涉及规定谁获得数字货币的鼓励、获得多少鼓励。当前,已有学者提出,应将全球资产映射为全球数字货币,从而帮助实现建立在区块链基础上的全球治理。¹上链资产并不一定表现为有形资产,全球治理参与者的参与资格、国际声望和国家信用等无形资产同样可以和智能合约联通并被作为奖惩手段,保证链基治理有效运行。

再次,把握验证机制作为全球治理监督机制的意义。区块链的共识机制设计对全球治理实践中的监督有重要意义,去中心化的监督意味着某种程度的全球民主,具备公平性然而效率低下;多中心化的监督意味着全球范围内的代议制,谁去实施监督职能,以及如何对被选举出来的监督人进行监督,将会引起关于全球正义和全球公平的争论;完全中心化的监督方式,则意味着高效,但同时也将给全球治理民主化带来挑战。

如果说分布式数据库是区块链的表现形式,加密技术是区块链的安全基础,那么,共识机制就是区块链的核心和灵魂。借助链下治理工具能动地把握以共识机制为核心的区块链自治理,是国家参与引领链基治理的突破口。具体而言,确保安全性是国家借助区块链参与和引领全球治理的底线。在此前提下,国家应对进行中的和潜在的链基治理实践的去中心性和效率进行权衡。例如,在相对弱势领域,可强调区块链的去中心性;在相对优势领域,则强调加强区块链的治理效率。只有通过创造性的和针对性的共识机制设计,才能保证区块链这一全球电子社会契约向着遏制强权、维护安全的方向发展。在对各种区块链共识机制研究的基础上,在不同的应用领域对前述“三元悖论”进行有针对性的调节,并制定相关国际规则,是国家的重要挑战和课题。

共识机制是区块链的核心和灵魂,借助链下治理工具把握以共识机制为核心的区块链自治理,是国家参与引领链基治理的突破口。

四、结语

自2020年下半年以来,区块链技术的发展再次迎来一股热潮,与前几次热潮不同,这股热潮背后是一批区块链实践应用项目的落地。在这一股应用落地热潮中涌现的分布式存储和分布式预言机,预示着链基治理的乐观前景。链基治理给处于困境中的全球治理提供了一条技术路径,即通过全球电子社会契约完善全

1 高奇琦:《主权区块链与全球区块链研究》,《世界经济与政治》,2020年第10期,第50—71页。

球治理机制。在全球电子社会契约面前，现有国际组织面临着功能转型的挑战，非政府组织和次国家行为体有望获得更多的机遇，国家将在获得新筹码的同时面临新的压力。对于国家来说，通过链下治理规范区块链的自治理，进而驾驭链基治理，是化解压力赢取筹码的路径，其核心在于对共识机制的把握。